ПРАВО НА ЦИФРОВУЮ БЕЗОПАСНОСТЬ: путеводитель по безопасному интернету для детей и их родителей

Брошюра подготовлена в рамках проекта
«Цифровая безопасность»,
реализуемого при поддержке
Благотворительного фонда «Дорога к дому»
компании «Северсталь»

г. Ярославль
2020

ПРЕДИСЛОВИЕ

Брошюра направлена на развитие компетенций школьников и их родителей в вопросах цифровой безопасности. Содержание брошюры нацелено на формирование у школьников и их родителей знаний, необходимых для понимания особенностей работы в интернет-пространстве, правовых основ пользования интернетом, ключевых правил поведения в цифровой среде и общих правил использования цифровых устройств.

Брошюра состоит из пяти разделов:

• что такое «право детей на цифровую безопасность», и как оно обеспечивается?;

• безопасный интернет для детей: базовые правила поведения в цифровой среде;

• цифровая памятка родителям;

• case-study в обучении детей технике цифровой безопасности;

• материалы по цифровой безопасности детей и подростков.

В разделах раскрываются понятия, связанные с «цифровой безопасностью», рассматриваются правовые основы обеспечения цифровой безопасности детей. Авторами определяются основные угрозы для цифровой безопасности детей, приводится ряд правил цифровой безопасности, которые важно разъяснять детям.

Отдельным блоком описаны советы родителям по обеспечению безопасности ребенка в интернете и безопасному использованию социальных сетей. Также в брошюре представлены общие правила использования цифровых устройств, разобраны ситуации по обучению детей технике цифровой безопасности, предложены полезные материалы по цифровой безопасности детей и подростков

Проект «Цифровая безопасность» реализуется Фондом поддержки социальных проектов и инициатив «Добрый город», при финансовой поддержке Благотворительного фонда «Дорога к дому» компании «Северсталь» и направлен на формирование у школьников и педагогов навыков безопасного поведения в сети интернет.

ЧТО ТАКОЕ «ПРАВО ДЕТЕЙ НА ЦИФРОВУЮ БЕЗОПАСНОСТЬ», И КАК ОНО ОБЕСПЕЧИВАЕТСЯ?

Цифровая безопасность – это комплекс мер, направленных на защиту конфиденциальности, целостности и доступности информации от случайных или преднамеренных воздействий естественного или искусственного характера, влекущих за собой нанесение ущерба владельцам или пользователям информации.

Цифровую безопасность детей можно определить как состояние защищенности ребенка и устройств, которыми он пользуется в цифровой среде. Обеспечению безопасной цифровой среды служит установление правил и применение мер предотвращения атак через информационно-телекоммуникационные сети.

Право на цифровую безопасность включает в себя право на обеспечение защиты информации от неправомерных действий, право на доступ к информации, а также право на конфиденциальность персональных данных в интернет-среде.

Основную угрозу для цифровой безопасности детей представляют:

1) мошенничество;
2) утечки персональных данных;
3) поддельные сайты, с помощью которых злоумышленники пытаются завладеть паролями или данными банковских карт;
4) взломы страниц в социальных сетях;
5) получение нарушающей законодательство информации;
6) разглашение информации личного характера;
7) онлайн-слежка за ребенком.

Цифровая безопасность детей обеспечивается следующими средствами:

1) правовые средства – через определение типов ограниченной и запрещенной к распространению информации, а также мер ответственности за нарушение правовых норм;
2) институциональные средства – через систему органов, имеющих

полномочия в сфере безопасности детей в интернете (суды, Роскомнадзор и пр.);

3) технические средства – через разработку и внедрение технических средств противодействия цифровым угрозам (антивирусные программы, программы-фильтры, аппаратные средства контроля).

Правовые основы обеспечения цифровой безопасности детей представлены в следующих нормативных актах:

1. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» – определяет виды информации, причиняющей вред здоровью и развитию детей; вводит классификацию информационной продукции и содержит требования к ее обороту.

Виды информации,
причиняющей вред здоровью и (или) развитию детей

Информация, запрещенная к распространению среди детей:

• побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству либо жизни и (или) здоровью иных лиц, либо направленная на склонение или иное вовлечение детей в совершение таких действий;

• способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, никотинсодержащую продукцию, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

• обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным;

• содержащая изображение или описание сексуального насилия;

• отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи;

• оправдывающая противоправное поведение;

• содержащая нецензурную брань;

• содержащая информацию порнографического характера;

• о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и

видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего.

Информация, ограниченная к распространению среди детей:

- представляемая в виде изображения или описания жестокости, физического и (или) психического насилия (за исключением сексуального насилия), преступления или иного антиобщественного действия;
- вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;
- представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;
- содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

2. Закон Российской Федерации от 27.12.1991 № 2124-1 «О средствах массовой информации» – устанавливает запрет на распространение определенного рода информации, которая может нести в себе запрещенные данные, в том числе данные, которые могут негативно сказаться на психике ребенка.

Так, в СМИ, в том числе в сетевых изданиях запрещено размещение:

- информации, за распространение которой следуют меры уголовной или административной ответственности, например, публичное распространение под видом достоверных сообщений заведомо ложной информации об эпидемиях, чрезвычайных экологических ситуациях, раскрытие врачебной тайны;
- материалов, которые содержат публичные призывы к осуществлению террористической деятельности или публично оправдывают терроризм, а также иные экстремистские материалы;
- материалов, пропагандирующих порнографию, культ насилия и жестокости, содержащих нецензурную брань;
- рецептов и мест приобретения наркотиков, их аналогов, прекурсоров и т.д.

Запрет распространения указанных видов информации обоснован тем, что еще не сформировавшая психика ребенка весьма восприимчива,

и доступность обозначенного рода информации может негативно сказаться на формировании личности ребенка, сформировать в нем негативные наклонности.

3. Федеральный закон от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации» – содержит запреты распространения определенных видов информации и положения, обязывающие власти предпринимать меры по защите ребенка от информации, пропаганды, агитации, которые могут нанести вред здоровью ребенка, его нравственному и духовному развитию.

В соответствии с этим законом, запрещена к распространению информация:

- направленная на разжигание классовой, национальной, социальной нетерпимости;
- реклама алкогольной продукции и табачных изделий;
- пропагандирующая социальное, расовое, национальное, религиозное неравенство;
- порнографического характера;
- пропагандирующая нетрадиционные сексуальные отношения;
- пропагандирующая насилие и жестокость, антиобщественное поведение, наркоманию.

В целях обеспечения безопасности жизни, охраны здоровья, нравственности ребенка, защиты его от негативных воздействий проводится экспертиза (социальная, педагогическая, психологическая) компьютерных игр и т.д.

Нарушение вышеобозначенных запретов распространения информации в интернете является основанием для привлечения виновных лиц к административной ответственности, предусмотренной в т.ч., положениями ст. 6.17 КоАП РФ, а также уголовной ответственности в соответствии с Уголовным кодексом РФ. Доступ к интернет-ресурсам, на которых размещена запрещенная к распространению среди детей информация, может быть ограничен.

БЕЗОПАСНЫЙ ИНТЕРНЕТ ДЛЯ ДЕТЕЙ: ГЛАВНЫЕ ПРАВИЛА ПОВЕДЕНИЯ В ЦИФРОВОЙ СРЕДЕ

Ниже приводится ряд правил, которые важно разъяснять детям по вопросам их цифровой безопасности.

1. Храни тайны!

Важно разъяснить ребенку недопустимость введения своих персональных данных на непроверенных сайтах. Регистрацию на сайтах, где необходимо ввести персональные данные, желательно проходить под присмотром родителей.

2. Сохраняй анонимность!

В профиле в социальных сетях ребенку следует указывать минимум информации о себе. Нежелательно указывать адреса, номера телефонов, дату рождения, школу, класс обучения.

3. Не переписывайся с незнакомцами!

Ребенок должен знать, что в интернете он может столкнуться с мошенниками, которые стремятся завладеть его данными или попытаться втянуть в сомнительную авантюру.

Главное средство защиты в этом случае – конфиденциальность! Для этого важно ограничить доступ к персональным данным и фотографиям ребенка.

4. Распознай мошенника!

Ребенку важно объяснить, что, если незнакомый человек, у которого закрытый профиль, мало друзей в социальной сети, отсутствуют фотографии на странице, просит прислать какую-либо информацию, не нужно выполнять такие просьбы, и следует добавить такое лицо в «черный список».

5. Сохраняй свои фотографии!

Для того чтобы фотография ребенка не стала достоянием общественности, не стоит выкладывать ее в интернет или отправлять посредством мессенджеров, поскольку они копируют переписку в «облако», и в этом случае можно потерять контроль над своими фотографиями.

Категорически нельзя выкладывать фотографии документов!

6. Особое внимание – компьютерным играм!

В играх нужно вести себя особенно осторожно, поскольку в игре ребенком проще манипулировать за счет членства в командах, внутриигровых связей, игровых объектов. Важно научить ребенка не идти на поводу у тех, кто пытается им манипулировать!

7. Распознай поддельный сайт!

Существуют сайты, которые являются способом выманивания у человека его логина, пароля, данных учетной записи (фишинг). Ребенку важно знать, что доверять следует только проверенным сайтам, и перед тем, как ввести пароль и логин, рекомендуется проверить адресную строку.

8. Используй разные пароли!

Для каждой учетной записи важно использовать свой пароль. Пароль должен быть надежным (не стоит использовать в качестве пароля дату своего рождения, Ф.И.О., номер телефона), это должна быть хаотичная комбинация цифр и букв.

9. Интернет-покупки – только с родителями!

Ребенок должен понимать, что покупки в интернет-магазинах желательно совершать только под присмотром взрослых. Все сервисы, которые принимают деньги, должны иметь протокол https и зеленый значок рядом. Если такой значок отсутствует, покупку лучше не совершать.

10. Не делай в интернете того, что запрещено в физическом мире, ведь разница между реальной и виртуальной действительностью – минимальна!

Ребенку важно объяснить основные правила поведения в интернете и то, какой контент является запрещенным к распространению. В интернете следует воздерживаться от оскорблений, пиратства и других запрещенных действий.

Не допускается выкладывать запрещенный контент, участвовать в травле, распространять чужую информацию в сети.

Важно разъяснить, что за совершение указанных выше действий следует ответственность.

Соблюдая эти простые правила, вы сможете обезопасить себя и своих детей от нежелательных ситуаций и негативных последствий!

ЦИФРОВАЯ ПАМЯТКА РОДИТЕЛЯМ

Общие правила использования цифровых устройств

Говоря о безопасности, пусть даже и цифровой, прежде всего, стоит сказать о самом главном – о здоровье ребенка, использующего цифровые устройства. Всемирная организация здравоохранения не могла оставить столь важную часть жизни современного ребенка без внимания и уже давно разработала нормы безопасного использования гаджетов.

Обратите внимание! Подобные требования адресованы в первую очередь родителям. Рассчитывать на то, что ваш ребенок проявит сознательность и будет соблюдать их без вмешательства старших, весьма опрометчиво.

Важно знать. Место, где ребенок использует устройство, должно быть достаточным образом освещено, изображение на экране должно быть четким, контрастным и не давать бликов. Оптимальное расстояние от глаз до экрана 55-60 см. Между небольшим экраном смартфона и более крупным планшета или компьютера стоит отдавать предпочтение второму.

Согласно требованиям СанПиН, для детей разного возраста предусмотрена разная продолжительность непрерывного взаимодействия с компьютером (Таблица 1).

Таблица 1

Возраст	Продолжительность непрерывной работы за компьютером
Дошкольный	7-10 минут
8-10 лет	45 минут
11-13 лет	1 час 30 минут
14-16 лет	2 часа 15 минут

Родителям стоит обратить внимание не только на продолжительность нахождения ребенка за компьютером, но и на признаки так называемой компьютерной усталости, которые могут начаться раньше обозначенного в таблице времени.

Признаки компьютерной усталости у ребенка:

- потеря контроля над собой: ребенок часто трогает лицо, сосет палец, гримасничает, кричит и т.п.;
- потеря интереса к компьютеру: ребенок часто отвлекается, вступает в разговоры, обращает внимание на другие предметы, не желая продолжать работу;
- «утомленная» поза: ребенок склоняется то в одну, то в другую сторону, откидывается на спинку стула, задирает ноги, упираясь в край стола;
- эмоционально-невротическая реакция: крик, подпрыгивания, истерический смех и др.

Обратите внимание! При наличии хотя бы одного из вышеуказанных признаков следует прекратить работу за компьютером или сделать длительный перерыв.

Как родителям обеспечить безопасность ребенка в интернете?

В вопросах поведения вашего ребенка в сети нужно быть наиболее осторожным. С одной стороны, вы рискуете нарушить тонкий внутренний мир подростка, с другой стороны, ребенок рискует наткнуться на взрослый контент, мошенничество, преступную деятельность.

Рекомендации по безопасному использованию социальных сетей

Несмотря на очевидную привлекательность, необходимо осознавать и опасности использования социальных сетей в раннем возрасте. Известно, что у детей планка критичного отношения к новостям, видео и сообщениям ниже, чем у взрослых. Дети более доверчивые, а значит, они удобный объект для воздействий.

Совершенно бесполезно ограждать ребенка от социальных сетей. Такое поведение вызовет лишь агрессию, непонимание и недоверие со стороны ребенка, ведь многие из его сверстников также активно используют социальные сети.

Важно знать. Нельзя четко назвать определенный возраст, начиная с которого ребенок может пользоваться социальными сетями. Если он желает создать страничку в социальной сети, нет смысла запрещать ему это. Важнее и полезнее не терять авторитет в глазах ребенка, а напротив, поддержать его и дать ряд наставлений.

Советы родителям

Что сделать для обеспечения безопасности:

• попросите ребенка общаться в социальной сети так, как будто его будет читать его учительница по русскому языку. Иначе все то, что ребенок изучает в школе, так и останется только в школе;

• ребенку стоит объяснить, что он несет ответственность за все, что пишет. Даже если подросток заводит аккаунт не от своего имени, то все равно должен контролировать те вещи, которые пишет и которыми делится. Анонимность – не уход от ответственности. Если ты не готов публиковать что-то под своим именем, значит, лучше не публиковать это вовсе;

• обратите внимание ребенка на то, что он должен аккуратно относиться и к той информации, что ему присылают друзья по переписке. Если ребенку прислали фотографию в личных сообщениях, это не значит, что он вправе публиковать её у себя на странице;

• на странице должно быть не больше той информации, которую ребенок не постесняется сказать незнакомцу. Должно быть понимание того, что нельзя все выставлять напоказ. А чтобы не показывать больше, чем нужно, стоит объяснить ребёнку, что такое настройки приватности. Предоставьте доступ к записям только друзьям и отключите возможность делиться фотографиями;

• можно завести аккаунты в тех же социальных сетях, подписаться на ребёнка и отслеживать, что он публикует и комментирует, какие фотографии размещает, кого добавляет в друзья, какую музыку слушает.

Что делать не нужно:

• строго запрещать ребенку общаться в социальных сетях, отбирать гаджеты и наказывать. Такое поведение приведет к агрессии и непониманию и лишь усилит желание использовать социальные сети;

• читать переписки ребенка, ругать его за них. Учитесь доверять своему ребенку, не стоит переживать по пустякам и без повода читать его переписку.

Обратите внимание! Современному родителю стоит обратить внимание и на свою страничку в социальной сети. Важно внимательно относиться к публикации любой информации, связанной с ребенком.

Родители, которые не только публикуют фотографии, но и его полное имя, дату и место рождения, сами отдают идентификационную информацию детей в руки мошенников. Американский еженедельник The New Yorker сообщает, что к 2030 году шерентинг[1] может стать

[1]Шерентинг - новый термин (от английского слова «parenting» - воспитывать и глагола «to share» - делиться, размещать в интернете), обозначающий процесс публикации родителями фотографий ребенка и иной информации о нем в социальных сетях.

причиной 2/3 случаев мошенничества с использованием персональных данных сегодняшних детей.

Советы родителям по использованию личных страниц в социальных сетях

Что сделать для обеспечения безопасности:

- проверьте настройки безопасности в социальной сети;
- предоставьте доступ к своим записям только друзьям и отключите возможность делиться вашими фотографиями;
- поговорите с друзьями и родными о конфиденциальности: попросите их не делиться вашими фотографиями;
- не добавляйте к фотографиям GPS-координаты, чтобы никто не мог определить местоположение вашего ребенка по фотографии;
- не указывайте данные, которые посторонние люди могут использовать для идентификации вашего ребенка – полное имя, дату рождения, номер школы;
- используйте никнеймы и образные выражения, которые не позволят незнакомцам установить личность вашего ребенка;
- пересмотрите список друзей и удалите из него случайных людей.

Что делать не нужно:

- «открывать» свою страницу, тем самым предоставляя доступ к ней для всех желающих;
- указывать геолокацию на фотографиях;
- размещать персональные данные о вас и вашем ребенке.

К сожалению, не только социальные сети могут принести негатив в жизнь вашего ребенка в сети интернет. Далее мы обозначим самые распространённые угрозы, способные негативным образом повлиять на вашего малыша, и предложим методы борьбы с ними.

Рекомендации по противодействию нежелательному контенту

К нежелательному контенту могут относиться сцены насилия, порнография, причинение вреда животным.

К сожалению, рано или поздно ваш ребенок столкнется с контентом подобного типа, как бы вы ни старались это предотвратить. В силах родителя сделать так, чтобы это не случилось слишком рано, а в уже сознательном возрасте не оставило отпечатка на психике.

Советы родителям

Что сделать для обеспечения безопасности

Установить «Родительский контроль». Про установку такого контроля на персональном компьютере или ноутбуке можно узнать у своего провайдера.

Существуют различные программы, которые ограничивают доступ к подозрительным сайтам, помогают контролировать действия и безопасность детей в сети и лимитируют время пребывания в интернете.

Можно ограничить доступ к социальным сетям, Youtube и другим платформам в часы занятий. Так ребёнок точно не станет отлынивать от просмотра уроков.

Что делать не нужно

Наказывать за обнаруженный нежелательный контент. Например, если вы обнаружили в истории браузера порнографию, не ругайте сына или дочь, спокойно поговорите об этом.

Рекомендации по противодействию кибербуллингу (травле)

Если ребёнок становится агрессивным, злым, раздражённым или дёрганым после общения в сети, это может быть признаком травли или конфликтов. Возможно, он подвергается психологическому давлению, издевательствам или угрозам в интернете.

Советы родителям

Что сделать для обеспечения безопасности:

- прежде всего, стоит пообщаться с ребенком, дать понять, что вы на его стороне, выяснить причины травли;
- далее стоит показать ребенку, как пользоваться блокировкой или «черным списком»;
- если в травле вашего ребенка участвуют ученики его школы, то необходимо сообщить об этом учителю и школьному психологу;
- в том случае, если вашему ребенку поступают угрозы и возникает опасение за его жизнь и здоровье, то соберите все переписки (скриншоты, фотографии) и обратитесь в правоохранительные органы.

Что делать не нужно:

- не стоит маниакально контролировать все социальные сети ребёнка, особенно читать переписки;

• чем старше сын или дочь, тем острее воспринимается ваше вторжение в личное пространство;

• чрезмерный контроль за безопасностью ребёнка в сети может оттолкнуть детей от вас;

• стройте отношения на доверии. Обучайте ребёнка правилам безопасного поведения в интернете и соблюдайте их сами.

Рекомендации по противодействию преступным посягательствам в интернете

Под киберпреступностью понимают целый ряд нарушений закона – от вымогательства личных данных до вовлечения несовершеннолетних в торговлю наркотиками.

Советы родителям

Что сделать для обеспечения безопасности:

• учите ребёнка здравому смыслу. Он должен понимать, что некоторые вещи – например, имена и должности родителей, адрес, пароль от социальной сети и так далее – нельзя никому раскрывать. Объясните, что интернет позволяет любому человеку выдавать себя за кого угодно. Перед тем как встретиться с другом, которого нашёл в сети, лучше поговорить со взрослыми;

• установите антивирус. Он будет блокировать подозрительные программы, которые ребёнок может нечаянно скачать на компьютер. Ими нередко пользуются хакеры, чтобы получить доступ к персональным данным. Кроме того, антивирус предупредит ребёнка о переходе по подозрительной ссылке, которая может позволить мошеннику дистанционно управлять устройством пользователя;

• в случае если ваш ребенок уже стал жертвой преступления, незамедлительно обратитесь в правоохранительные органы.

Что делать не нужно:

• относиться к проблеме несерьезно, так как это чревато не только финансовыми потерями, но и угрожает жизни и здоровью вашего ребенка;

• жалеть деньги на лицензионные антивирусные программы;

• пользоваться нелицензионным программным обеспечением, в том числе, и операционной системой;

• пытаться решить проблему самому в том случае, если она уже есть.

Важно знать. Обеспечить безопасность детей в интернете важно, но стоит быть реалистами: никогда не получится создать волшебный мыль-

ный пузырь и оградить ребёнка от всего плохого, что существует в мире.

Рано или поздно дети в интернете сталкиваются и с нежелательным контентом, и со страшными фильмами.

Не забывайте: именно вы создаете цифровой след вашего ребенка.

Чем крепче всемирная паутина связывает нас, тем выше ответственность родителей.

Проследить за цифровым следом ребенка так же важно, как дать ему хорошее образование и воспитать в нем сознательного гражданина.

Делая это, вы не просто добросовестно исполняете родительские обязанности, вы показываете детям, что вы их любите.

CASE-STUDY В ОБУЧЕНИИ ДЕТЕЙ ТЕХНИКЕ ЦИФРОВОЙ БЕЗОПАСНОСТИ

Для того, чтобы дети усвоили правила безопасного поведения в интернете, нужно продемонстрировать ту или иную проблему и найти ее решение. Найдя оптимальный вариант действий в конкретной ситуации, школьники смогут проецировать выход и из других проблемных ситуаций, связанных с цифровой безопасностью.

Решением этой задачи служат кейсы, содержащие описание гипотетических событий, которые могут произойти в интернете. Разбор таких заданий с родителями и учителями поможет разъяснить детям основные аспекты безопасного поведения в сети.

Ниже приводятся некоторые варианты кейсов, которые мы предлагаем к обсуждению с детьми старших классов.

? Кейс 1

На концерте, приуроченном к Дню защиты детей, ученица 9 класса Мария вела съёмку происходящего на фото и видеокамеру. Помимо самой Марии, в кадр попал зритель Сидоров. Мария поделилась фото и видеозаписью в социальных сетях.

Спустя некоторое время Сидоров обнаружил в интернете пост Марии, на котором было запечатлено его изображение. Крайне возмутившись увиденным, Сидоров потребовал у Марии удалить все опубликованные материалы с его участием. Мария отказалась, сославшись на то, что это ее фотографии и видео.

Оцените ситуацию.

Решение кейса 1

Для решения кейса следует обратиться к статье 152.1 Гражданского кодекса РФ (далее – ГК РФ), согласно которой обнародование и дальнейшее использование изображения гражданина (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, в которых он изображен) допускаются только с согласия этого гражданина.

Из этого правила имеются исключения.

Согласие на обнародование и использование изображения гражданина не требуется в следующих случаях:

1. если использование изображения осуществляется в государственных, общественных или иных публичных интересах;
2. если изображение гражданина получено при съемке, которая проводится в местах, открытых для свободного посещения, или на публичных мероприятиях (собраниях, съездах, конференциях, концертах, представлениях, спортивных соревнованиях и подобных мероприятиях), за исключением случаев, когда такое изображение является основным объектом использования;
3. если гражданин позировал за плату.

В условии кейса указывается, что съемка происходила на концерте. В силу прямого указания подпункта 2 пункта 1 статьи 152.1 ГК РФ, концерт относится к мероприятиям, на которых допускается проведение съемки с возможностью обнародования и дальнейшего использования изображений зрителей без необходимости получения их согласия. Следовательно, Мария не должна удалять свой материал, так как согласие возмущенного Сидорова не требовалось.

Однако нужно разъяснить, при каких условиях фотоснимок, сделанный на публичном мероприятии, можно разместить только с согласия того, кто на нем изображен.

В пп. 2 п. 1 ст. 152 ГК РФ говорится о данном исключении – когда изображение является основным объектом использования. И поэтому, если изменить условие нашего кейса и предположить, что изображение Сидорова является основным объектом использования, для размещения его фотографии потребуется его согласие.

Обратите внимание! Для более простого объяснения школьникам материала и лучшего усвоения задачи рекомендуем задавать им наводящие вопросы. Предложите более простые ситуации и попросите оценить их с точки зрения допустимого или противоправного поведения. Например, спросите, нужно ли просить согласие, когда делаешь селфи на концерте. Это покажется им абсурдным, но так или иначе, вы вместе доберетесь до истины.

Кейс 2

Морозов зашел на сайт интернет-магазина, который уведомил его об использовании файлов cookie. Морозову было предложено либо согласиться с данным условием работы с сайтом, либо покинуть его без возможности дальнейшего использования интернет-магазина. Форма согласия была сформирована автоматически, с автоматическим проставлением галочки в графе «согласен». Полагая, что действия сайта противоречат действующему законодательству, Морозов обратился за юридической консультацией.

Оцените ситуацию.

Решение кейса 2

Начиная разбор предоставленной нами ситуации, стоит ответить на вопрос о том, что представляют из себя файлы cookie.

Однозначного ответа на этот вопрос в законодательстве нет, однако под ними понимают текстовые файлы небольшого объема со служебной информацией для браузера. Иными словами, сервер обменивается с веб-обозревателем на ПК или мобильном гаджете данными о сайтах, которые посещал пользователь. Информация может быть разнообразной, например, в таких файлах хранится статистика посещений, логины пароли от сайтов или сервисов, индивидуальные настройки пользователя (регион, дизайн оформления и прочее).

Вышеуказанная информация, содержащаяся в файлах cookie, в руках злоумышленников может сильно нам навредить, поэтому, посещая интернет-порталы, нужно обладать определенными базовыми правовыми знаниями.

Во-первых, согласно статье 3 Федерального закона «О персональных данных», персональные данные – это любая информация, относящаяся к прямо или косвенно определённому, или определяемому физическому лицу (субъекту персональных данных).

Исходя из данного определения, мы можем сделать вывод о том, что cookie-файлы, обрабатывая информацию о посещениях определенных интернет-порталов, местоположении пользователя, логинах и паролях от сайтов, непосредственно взаимодействуют с персональными данными.

Во-вторых, в соответствии со статьей 2 этого же закона, его целью является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты права на неприкосновенность частной жизни, личную и семейную тайны.

В-третьих, в силу правовой позиции Конституционного суда РФ, выраженной в Определении от 09.06.2005 № 248-0, право на неприкосновенность частной жизни означает предоставление и гарантию человеку

возможности контролировать информацию о самом себе, препятствовать разглашению сведений личного, интимного характера.

Из всего этого можно сделать вывод о том, что в описанном случае интернет-магазин, запрещая использовать сайт при несогласии на использование файлов cookie, нарушает права Морозова, которому для посещения сайта необходимо принудительно согласиться на обработку персональных данных. Все это, в свою очередь, несовместимо с принципом свободы поиска, получения, передачи, производства и распространения информации.

Обратите внимание! Кейс рекомендуется разбирать со школьниками более старшего возраста. Следует иметь в виду, что в большинстве случаев они не понимают, что такое файлы cookie и чем они могут навредить, рекомендуется использовать иллюстрации и, возможно, более простые примеры.

Кейс 3

К вам приехал погостить дальний родственник. Пока вас нет, родственник решил воспользоваться вашим компьютером для того, чтобы скачать через торрент музыку для телефона. Вернувшись, вы увидели, что он ругается, что ничего не работает, закрывает предупреждение антивируса и запускает явно вирусную программу.

Что необходимо предпринять, чтобы минимизировать ущерб от действия этого вируса?

Решение кейса 3

Чтобы разрешить описанную в кейсе проблему, необходимо, прежде всего, отключить интернет. Дело в том, что вирус может не активироваться без полного скачивания, кроме того, ряд вирусов работает только при подключении к сети интернет. Следовательно, отключение интернета поможет минимизировать вред от действия вируса.

После этого рекомендуется запустить проверку антивируса. В настоящее время в базе данных огромное количество видов вирусов, и практически любой антивирус найдет угрозу. Можно также воспользоваться ручной проверкой через диспетчера задач. Искать надо новые и/или подозрительные процессы.

Кроме того, имеет смысл проверить автозагрузку компьютера. Вирус мог попасть туда, чтобы запускаться каждый раз при включении компьютера.

Когда антивирус закончит проверку и ручная проверка покажет, что подозрительных процессов нет, следует перезагрузить компьютер и вы-

полнить проверку еще раз, чтобы проверить отсутствие вируса. При этом нужно помнить, что наши данные могли уже быть отправленными злоумышленником, и чтобы обезопасить себя, нужно сменить пароль.

Обратите внимание! При общении со школьниками стоит в ходе объяснения показывать иллюстрации, чтобы они наглядно могли понять, о чем идет речь. Зачастую дети знакомы с инструментами, с помощью которых можно разрешить проблему, но не знают, что их можно использовать для данной цели.

МАТЕРИАЛЫ ПО ЦИФРОВОЙ БЕЗОПАСНОСТИ ДЕТЕЙ И ПОДРОСТКОВ

Современные технологии могут содержать не только угрозы для цифровой безопасности, но и открывать широкие возможности для обучения детей в этом направлении. И этими возможностями мы рекомендуем активно пользоваться. Ниже будет приведен перечень полезных для детей и родителей цифровых сервисов и интернет-ресурсов, обучающих базовым правилам интернет-защиты.

1. Справочно-игровой сервис SkillCity.

Как известно, любая информация легче воспринимается в формате игры, и, несомненно, для самих детей такой способ будет намного лучше и приятнее. С этим прекрасно справляется такой сервис, как SkillCity.

Так выглядит главная страница указанного сервиса.

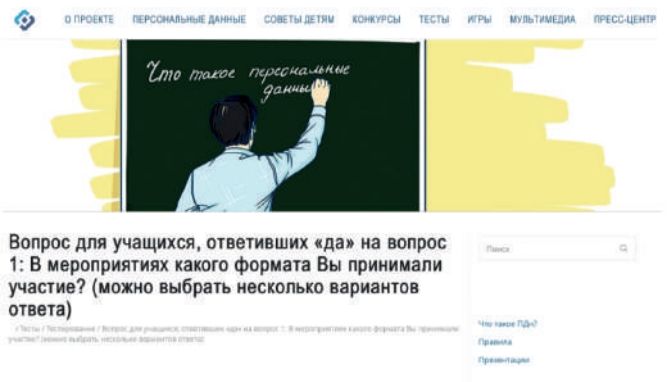
Найти его можно по адресу https://skillcity.ru/. Приложение сервиса до-

ступно в любом удобном для вас магазине приложений для смартфона, есть версия как для Android, так и для IOS.

Данный проект был разработан с целью предоставления информации о цифровом мире и о современных профессиях в доступном виде. Здесь вы можете найти мини-игры, проходя которые ребенок будет узнавать информацию о различных современных компаниях и профессиях нового времени, а также сможет приобрести совершенно разные, но при этом полезные навыки, которые помогут ему в будущем.

Интересный факт: в изначальном тестировании проекта участвовали сами дети, что делает данный сервис еще удобнее и комфортнее для восприятия молодой аудиторией.

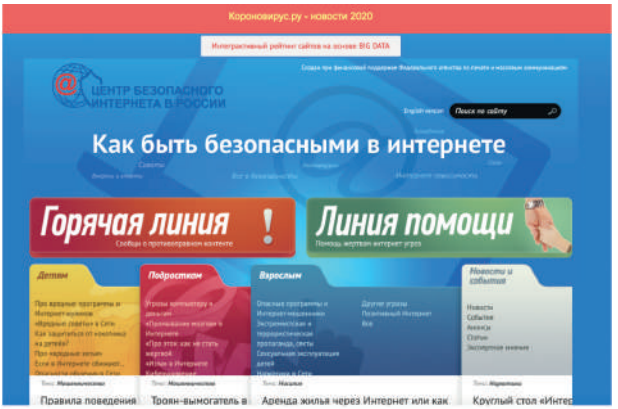
2. Следующим, не менее интересным сервисом, является **проект Роскомнадзора, посвященный защите персональных данных детей.**



Это главная страница данного проекта. А найти его в интернете можно по ссылке персональныеданные.дети. На сайте имеются советы для детей, конкурсы, различные тесты и игры.

На сайте собраны материалы, разработанные специалистами, для педагогов и родителей, которые желают учить и объяснять детям важность конфиденциальности личной жизни при использовании сетевых технологий. На данной интернет-площадке имеется много различной информации о том, какие последствия информационные технологии могут оказать на личную жизнь, а также множество инструментов, помогающих выработать необходимые навыки при принятии решений в вопросах виртуальной жизни.

3. Ресурс Центра безопасного интернета в России.



Так выглядит главная страница данной площадки, найти которую можно по ссылке https://www.saferunet.ru/.

На сайте имеются разделы с информацией для детей, подростков и взрослых людей. Там собраны материалы, посвященные цифровой безопасности и разумному поведению в сети интернет. Также на данной странице представлены «горячая линия» и «линия помощи», через которые можно сообщить о противоправном, нежелательном контенте и об интернет-угрозах.

Организаторами проекта являются Уполномоченный при Президенте РФ по правам ребенка, правозащитное движение «Сопротивление», Общественная палата РФ, РОЦИТ.

4. Брошюра, выпущенная отделением Майкрософт в России и СНГ.

Брошюра адресована не только родителям и педагогам, но и самим детям.

В ней простым и понятным языком рассказывается о том, как сделать работу и развлечение детей в интернете безопасными для них самих и других пользователей.

Брошюра рассказывает о том, как необходимо вести себя в сети интернет, каких правил стоит придерживаться, на что следует обращать свое внимание, а на что не стоит.

Дополнительно в ней представлены возрастные особенности детей при использовании всемирной паутины, правила интернет-этикета, рассказывается о технических средствах, которые могут использовать родители для повышения уровня безопасности малолетних пользователей.

Брошюру можно найти на сайте soprotivlenie.org.

Далее остановимся на разных технических средствах и программах, которые могут и должны применять родители для повышения уровня безопасности своих детей при использовании сети интернет.

На многих устройствах есть возможность установить функцию **Родительский контроль.**

С ее помощью можно:

- ✓ установить временные промежутки использования интернета;
- ✓ создавать «черный список» вредоносных сайтов и сервисов;
- ✓ использовать безопасный поиск по запрещенным словам;
- ✓ контролировать посещение интернет-ресурсов;
- ✓ получать отчет о посещенных страницах;
- ✓ удаленно просматривать экран компьютера, а также удаленно выключать и перезагружать его.

Основные способы родительского контроля

Родительский контроль у провайдера.

Как правило, данная услуга является платной и, к сожалению, доступна не у каждого поставщика интернет-услуг. Чтобы узнать о том, есть ли у вашего провайдера данная функция, следует обратиться к провайдеру по телефону или через Личный кабинет.

Функции родительского контроля, доступные во всех популярных антивирусах.

Обратите внимание! Указанный способ родительского контроля оправдан лишь при условии использования лицензионной версии антивирусной программы.

Иные способы

Родительский контроль как функция операционной системы Windows.

Владельцы ПК на базе ОС Windows имеют возможность бесплатно установить и использовать программу Family Safety («Семейная безопасность») из пакета Windows Essentials.

Обратите внимание! Указанный способ родительского контроля оправдан лишь при лицензионной версии операционной системы.

Родительский контроль в браузере.

Здесь можно использовать функцию родительского контроля в браузере Google Chrome или же бесплатное расширение для браузера Mozilla Firefox под названием Гогуль. Они блокируют нежелательный контент и помогают контролировать время, проведенное во всемирной паутине.

Родительский контроль с помощью смартфона.

На смартфонах можно установить программы с функцией родительского контроля (например, Kaspersky Safe Kids, Safe lagoon, Kids Place и др.), а также есть возможность подключить функцию «Детский интернет» у мобильного оператора.

Родительский контроль с помощью Wi-Fi роутера.

У некоторых роутеров есть встроенная функция Parental Control (Родительский контроль). Его настройка предоставляет возможность создавать правила доступа к сайтам для каждого компьютера или мобильного устройства, которое подключается через точку доступа (устройства распознаются по MAC-адресу). Можно также запретить доступ к определённым сайтам или разрешить только к некоторым для всех устройств, которые работают через один и тот же роутер.

Обратите внимание! Указанный способ родительского контроля оправдан лишь при использовании современных моделей Wi-Fi роутеров.

Специальное программное обеспечение.

Специальные программы для родительского контроля обладают рядом преимуществ перед остальными способами, так как предоставляют больший объем возможностей:

- ✓ анализ содержимого страниц на присутствие запрещенных слов;
- ✓ блокирование доступа к сайтам из «черного» списка;
- ✓ ограничение использования интернета по времени;

✓ просмотр экрана компьютера ребенка по сети (удаленная перезагрузка и выключение);
✓ режим «Безопасный поиск» в поисковых системах;
✓ запись адресов посещенных сайтов в файл-журнал;
✓ отсылка отчета о посещенных страницах по электронной почте;
✓ автоматическая деактивация программы для администраторов программы;
✓ специальные функции для работы с программой через локальную сеть;
✓ контроль запуска игр.

Список самых известных программ, позволяющих установить функцию родительского контроля:

1) Интернет-Цензор – является самой строгой программой и активно внедряется в учебных заведениях нашего государства;
2) Netpolice – выполняет отсев и фильтр сайтов по критериям: табак, компьютерные игры, онлайн-казино;
3) Сервис OpenDnS – не требует скачивания и обновления. Достаточно прописать в настройках сети определенные адреса DnS-серверов;
4) Один дома – программа-фильтр, защищает ребенка от негативной информации и взрослых сайтов, помогает ему самостоятельно изучать интернет-пространство;
5) K9 Web Protection – бесплатная программа для родительского контроля, блокирующая сайты по определенным категориям;
6) KinderGate Родительский контроль – программный продукт, предназначенный для домашнего использования и позволяющий контролировать использование сети интернет несовершеннолетними детьми и др.

Коллектив авторов и составителей брошюры:

Фролов Александр Альбертович – кандидат политических наук, руководитель проекта «Цифровая безопасность»;

Симонова Снежана Владимировна – кандидат юридических наук, руководитель Клуба цифрового права «Digital Femida»;

Арамянц Сюзанна Эдуардовна – студентка 3 курса юридического факультета ЯрГУ им. П.Г. Демидова;

Иванова Виктория Сергеевна – студентка 4 курса юридического факультета ЯрГУ им. П.Г. Демидова;

Кобяков Сергей Алексеевич – студент 5 курса математического факультета ЯрГУ им. П.Г. Демидова;

Смурков Иван Дмитриевич – студент 3 курса юридического факультета ЯрГУ им. П.Г. Демидова;

Шеломин Кирилл Юрьевич – студент 3 курса юридического факультета ЯрГУ им. П.Г. Демидова.

Брошюра составлена при поддержке:
Клуба цифрового права «Digital Femida» ЯрГУ им. П.Г. Демидова;
Уполномоченного по правам человека в Ярославской области;
Автономной некоммерческой организации
«Ресурсный центр поддержки НКО и гражданских инициатив».

Отпечатано: ИП Дурынин В.В.
г. Ярославль, проспект Машиностроителей, д. 83, оф.110
ИНН 760300624335
Тираж 1000 экз. 2020 г.